(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2003 (03.01.2003)

PCT

(10) International Publication Number
WO 03/001736 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/KR02/00288

(22) International Filing Date: 22 February 2002 (22.02.2002)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
2001-0035260 21 June 2001 (21.06.2001) KR

(71) Applicant *(for all designated States except US)*: **STAR-BRIDGE COMMUNICATIONS CO., LTD.** [KR/KR]; 254-8 Kongduk-dong, Mapo-ku, 121-020 Seoul (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CHO, Hui-Yol** [KR/KR]; 1424-401 Shinsikagi Apt., Mok-dong, Yangchun-ku, 158-050 Seoul (KR).

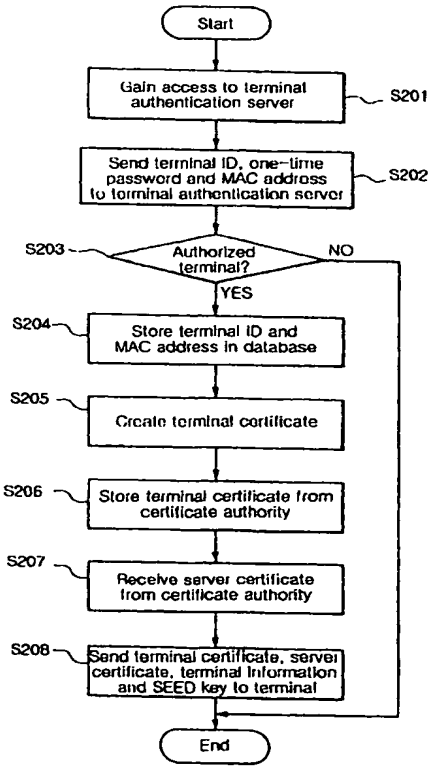
(74) Agent: **SON, Won**; C & S Patent and Law Office, C-2306 Daelim Acrotel, 467-6 Dogok-dong, Gangnam-ku, 135-270 Seoul (KR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

[Continued on next page]

(54) Title: METHOD FOR AUTHENTICATING SETTLEMENT TERMINAL AND SETTLEMENT METHOD USING THE SAME



(57) Abstract: A settlement method that provides a more reliable security effect. The settlement method comprises the step of entering initial terminal information to a settlement server (8) through a settlement terminal (3) and receiving a terminal ID and one-time password created by the settlement server, the step of sending the terminal ID and one-time password and a MAC address to the settlement server through the terminal, the step of determining that the terminal is an authorized one and then storing the terminal ID, one-time password and MAC address in the settlement server, the step of creating a terminal certificate for an SSL protocol encrypted in an RSA manner and storing the created terminal certificate in an LDAP server (7), and the step of sending the terminal information and terminal certificate, and a server certificate and SEED key created by a certificate authority (4) to the terminal.

WO 03/001736 A1

GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

METHOD FOR AUTHENTICATING SETTLEMENT TERMINAL AND SETTLEMENT METHOD USING THE SAME

Technical Field

The present invention relates to a method for authenticating a settlement terminal, and more particularly to a settlement terminal authentication method and a settlement method using the same, wherein settlement for a transaction can be prevented from being illegally conducted due to an information leakage occurring during transmission and reception of information for the transaction settlement through the use of a settlement terminal such as a credit card reader.

Background Art

Recently, with the ongoing industrialization and the advent of credit society, payment systems have been rapidly spread from a direct type where currency is paid directly for commodity purchasing or service use to an indirect type where money is paid through the use of a credit card, etc. for the commodity purchasing or service use. The indirect payment systems provide transparent transaction particulars enabling the prevention of problems such as tax evasion and so forth. In this regard, it is the current reality that the indirect payment systems are nationally widely encouraged.

In a conventional credit card-based settlement method, when a user purchases a commodity from a credit card-affiliated store or uses a service therefrom, a credit card reading terminal reads user information stored in a credit card of the user and sends the read information to a credit card company together with transaction records. Thereafter, the credit card company approves the transaction on the basis of the sent user information.

However, the above-mentioned conventional credit card-based settlement

method has an unsolved problem in that another person may make a fraudulent use of the user's credit card. Although the fraudulent use of the credit card mostly results from a loss or theft of the card, it may be sometimes caused due to a leakage of information being transmitted and received between the credit card reading terminal and the credit card company. For this reason, there is a need for user authentication to prevent the credit card from being illegally used by another person. Further, in order to prevent the credit card from being illegally used due to the information leakage, a settlement terminal must be authenticated for transaction settlement on the basis of encrypted data.

Disclosure of the Invention

Therefore, the present invention has been made in view of the above problems, and it is an object of the present invention to provide a method for authenticating a settlement terminal, wherein settlement for a transaction can be prevented from being illegally conducted due to an information leakage occurring during transmission and reception of information for the transaction settlement through the use of the settlement terminal.

It is another object of the present invention to provide a settlement method wherein a settlement terminal is authenticated for transaction settlement on the basis of a dually encrypted terminal certificate, thereby providing more reliable security of information.

In accordance with one aspect of the present invention, the above and other objects can be accomplished by the provision of a method for authenticating a settlement terminal connected to a settlement server over a network, comprising the steps of a) entering initial terminal information to the settlement server through the terminal and receiving a terminal ID and one-time password created by the settlement server; b) gaining access to the settlement server through the terminal and sending the terminal ID and one-time password and a MAC (Media Access Control) address to the

settlement server; c) determining on the basis of the sent terminal ID, one-time password and MAC address that the terminal is an authorized one and then storing the terminal ID, one-time password and MAC address in the settlement server; d) creating a terminal certificate for an SSL (Secure Socket Layer) protocol encrypted in an RSA (Rivest-Shamir-Adleman) manner on the basis of the terminal information and MAC address and storing the created terminal certificate in an LDAP (Light Weight Directory Access Protocol) server; and e) sending the terminal information and terminal certificate, and a server certificate and SEED key created by a certificate authority to the terminal.

Preferably, the above step a) may include the steps of a-1) connecting the terminal to the settlement server over the network; a-2) entering a user ID and password for user identification; a-3) sending the terminal information to the settlement server through the terminal if a user is an authorized one; a-4) storing the sent terminal information and creating the terminal ID and one-time password on the basis of the stored terminal information; and a-5) storing the created terminal ID and one-time password and sending the stored terminal ID and one-time password and the MAC address to the terminal.

In accordance with another aspect of the present invention, there is provided a settlement method based on authentication of a settlement terminal, comprising the steps of a) for settlement for a transaction, sending settlement information and a terminal certificate, encrypted on the basis of a SEED key, from the terminal to a settlement server according to an SSL (Secure Socket Layer) protocol over a network; b) extracting a terminal certificate and terminal information stored in an LDAP (Light Weight Directory Access Protocol) server; c) comparing a MAC (Media Access Control) address contained in the terminal certificate sent from the terminal with that contained in an information packet and, if the two MAC addresses are the same, determining that the terminal certificate sent from the terminal is valid; d) comparing the terminal certificate sent from the terminal with the terminal certificate extracted from the LDAP server and authenticating the terminal if the two terminal certificates are the same; and e)

approving the transaction on the basis of the settlement information and then sending approval information to the terminal.

Brief Description of the Drawings

The above and other objects, features and other advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram schematically showing a connection between a settlement terminal and a terminal authentication server over a network;

Fig. 2 is a block diagram illustrating a signal flow of an initial terminal information registration procedure of a settlement terminal authentication method in accordance with the present invention;

Fig. 3 is a flow chart illustrating the initial terminal information registration procedure of the settlement terminal authentication method in accordance with the present invention;

Fig. 4 is a block diagram illustrating a signal flow of a terminal authentication procedure of the settlement terminal authentication method in accordance with the present invention;

Fig. 5 is a flow chart illustrating the terminal authentication procedure of the settlement terminal authentication method in accordance with the present invention; and

Fig. 6 is a flow chart illustrating a settlement method in accordance with the present invention.

Best Mode for Carrying Out the Invention

In the present invention, a settlement terminal is authenticated on the basis of

encrypted data. The settlement terminal is a general credit card settlement terminal. This credit card settlement terminal is generally connected to a settlement server or financial institution via a dedicated line. In this regard, a specific dedicated line is required in a place where the settlement terminal is installed. In this invention, the settlement terminal must be registered and authenticated because it is connected to a very high speed Internet network (under a TCP/IP environment), such as an ISDN or ADSL. Over the Internet, the position and information of the terminal have to be verified for each settlement. As a result, the authentication is required each time a settlement is conducted.

Note that security of information is an essential factor to an open environment such as the Internet. In this connection, in the present invention, information is encrypted and transmitted and received for terminal authentication required for settlement. To this end, in the invention, modified SSL (Secure Socket Layer) communication is performed to exchange certificates between a server and a terminal on the basis of an asymmetric algorithm-based encryption. Further, the terminal encrypts information through the use of a symmetric algorithm-based SEED key and sends the encrypted information to the server. Although DES, 3DES and IDEA are generally used for symmetric encryption in a standard SSL, the present invention employs a modified SSL using SEED.

In addition, according to the present invention, a terminal authentication server creates a one-time password in an initial terminal information registration procedure such that the password is used for terminal authentication.

Now, a preferred embodiment of a settlement terminal authentication method according to the present invention will be described in detail in conjunction with the accompanying drawings.

With reference to Fig. 1, there are conceptually shown in block form connections from a settlement-dedicated terminal 3 to a terminal authentication server 5 and a settlement server 8 over a network 1.

As shown in Fig. 1, the settlement-dedicated terminal 3 is connected to the terminal authentication server 5 and settlement server 8 over the network 1, which may be a TCP/IP-based very high speed communication network (for example, an ADSL network). The terminal authentication server 5 is connected to an LDAP server 7, and the settlement server 8 is connected to a financial settlement server 9 and a financial institution 11. Although the terminal authentication server 5, LDAP server 7 and settlement server 8 are shown in Fig. 1 to be individual servers, they may be substantially included in one server, or a Web server of a settlement service provider.

The dedicated terminal 3, which is driven by a general or exclusive Web browser or an exclusive operating system, stores a SEED key provided from a certificate authority and encrypts information to be sent, using the stored SEED key. The terminal 3 is also adapted to exchange certificates with the terminal authentication server 5 according to a modified SSL protocol.

As stated previously, information read by the dedicated terminal 3 is dually encrypted through the SSL and SEED key (i.e., encrypted according to the symmetric algorithm and asymmetric algorithm) and then sent to the terminal authentication server 5 over the network 1. The LDAP (Light Weight Directory Access Protocol) server 7 acts to store terminal information and a server certificate authenticated by the certificate authority and provide the stored certificate and terminal information to the terminal authentication server 5 when the terminal 3 is required to be authenticated.

A description will hereinafter be given of an initial terminal information registration procedure in accordance with the present invention with reference to Fig. 2 which is a block diagram illustrating a signal flow of the initial terminal information registration procedure, and Fig. 3 which is a flow chart illustrating in detail the initial terminal information registration procedure.

For terminal registration, first, a manager dispatched from a terminal manufacturing company gains access to the terminal authentication server 5 through the terminal (S101) and enters an ID and password thereto (S102). The terminal

authentication server 5 receives the ID and password entered by the manager and compares them with those stored in a database 13 to determine whether the manager is an authorized one (S103). If the manager is an authorized one, the terminal authentication server 5 permits the manager to enter and send terminal information to the server 5 through the terminal 3 (S104). Thereafter, the terminal authentication server 5 receives the terminal information sent from the manager and stores it in the database 13 (S105).

Subsequently, the terminal authentication server 5 creates a one-time password in an existing 'challenge/response' manner or 'time synchronous' manner, which is well known in the art. The server 5 also creates a terminal ID (S106). The server 5 stores the created one-time password and terminal ID and a MAC (Media Access Control) address in the database 13 at the same time as sending them to the terminal 3 (S107).

Through the above-described procedure, the terminal information is stored and registered in the database of the terminal authentication server, and the dedicated terminal is provided with the terminal ID, one-time password and MAC address for terminal authentication from the terminal authentication server.

As stated above, the terminal authentication server 5 registers the terminal information, sent from the manager through the terminal, creates the terminal ID and one-time password and sends them back to the terminal. The terminal stores the terminal ID and one-time password sent from the terminal authentication server 5. Thereafter, for terminal authentication, the terminal gains access to the server 5 using the terminal ID and one-time password, and is then authenticated by the server 5.

The terminal authentication server 5 is preferably a Web server that verifies user information and transaction information, applied from the terminal 3 for transaction settlement, and transfers settlement information to the settlement server as a result of the verification to allow the settlement server to approve the transaction. That is, the terminal authentication server 5 authenticates a specific terminal existing on the Internet when settlement for a transaction is required, so that the transaction settlement can be conducted.

Next, a description will be given of a terminal authentication procedure in accordance with the present invention with reference to Fig. 4 which is a block diagram illustrating a signal flow of the terminal authentication procedure, and Fig. 5 which is a flow chart illustrating in detail the terminal authentication procedure.

For terminal authentication, first, the terminal 3 gains access to the terminal authentication server 5 (S201) and sends to the server 5 the terminal ID, one-time password and MAC address assigned upon the terminal registration (S202). The terminal authentication server 5 checks the terminal ID, one-time password and MAC address sent from the terminal to determine whether the terminal is an authorized one (S203). In the case where the terminal is an authorized one, the terminal authentication server 5 stores the sent terminal ID and MAC address in the database 13 (S204).

Thereafter, the terminal authentication server 5 creates a terminal certificate on the basis of the terminal information and MAC address (S205), and transfers the created terminal certificate to the LDAP server 7 to store it therein (S206).

It should be noted herein that the terminal certificate is created in an asymmetric algorithm-based RSA (Rivest-Shamir-Adleman) manner because the modified SSL communication can be performed between the terminal 3 and the terminal authentication server 5.

On the other hand, if the terminal authentication server 5 requests a server certificate from a certificate authority 4 for authentication thereof, then the certificate authority 4 creates the server certificate in response to the request from the server 5 and provides it to the server 5 (S207).

Thereafter, the terminal authentication server 5 sends the terminal certificate, server certificate, terminal information and SEED key to the terminal 3 (S208).

As stated above, according to the present invention, the terminal 3 receives the one-time password, created upon its registration, from the terminal authentication

server 5, accesses the server 5 on the basis of the received password and receives the created terminal certificate and server certificate from the server 5 again. At this time, the terminal 3 also receives the symmetric algorithm-based SEED key to be used for the SSL communication and encrypts information to be sent, using the received SEED key.

In the present embodiment, the terminal 3 is a general credit card reading terminal, preferably a settlement-dedicated terminal equipped with an exclusive Web browser (or exclusive operating system software).

The terminal certificate, terminal information and SEED key, provided upon the initial authentication of the terminal 3, are used for terminal authentication and encryption of information to be sent, when transaction settlement is actually conducted. Fig. 6 illustrates a settlement method according to the present invention, wherein transaction settlement is conducted on the basis of terminal authentication.

As shown in Fig. 6, if a user purchases a commodity or uses a service and then presents his/her credit card to settle his/her account for the commodity purchasing price or service usage fee (S301), the credit card reading terminal 3 encrypts the settlement information and terminal certificate with the SEED key and sends the encrypted settlement information and terminal certificate to the terminal authentication server 5 (S302). At this time, the settlement information includes the terminal information, information contained in the credit card, transaction records and so forth.

Notably, the terminal certificate is created according to the SSL protocol (namely, the RSA manner)-based asymmetric algorithm and then encrypted through the use of the symmetric algorithm-based SEED key. In other words, the terminal certificate is dually encrypted according to the symmetric/asymmetric algorithms, thereby ensuring more reliable security of information.

Thereafter, the terminal authentication server 5 requests the LDAP server 7 to transfer the terminal certificate stored therein (S303). The terminal authentication server 5 compares the MAC address contained in the terminal certificate sent from the

terminal 3 with that contained in an information packet to determine whether they are the same. In the case where the two MAC addresses are determined to be the same, the terminal authentication server 5 recognizes that the terminal certificate sent from the terminal 3 is valid. Subsequently, the terminal authentication server 5 compares the terminal certificate sent from the terminal 3 with that transferred from the LDAP server 7 to determine whether they are the same. If the two terminal certificates are determined to be the same, then the server 5 authenticates the terminal 3 (S304).

After authenticating the terminal 3, the terminal authentication server 5 transfers the settlement information to the settlement server 8 to request it to approve the transaction (S305). Upon receiving the settlement information (containing, for example, user information, a user ID, a password and transaction records) transferred from the terminal authentication server 5, the settlement server 8 compares the received settlement information with information stored in its database to determine whether the user is a valid one. If the user is determined to be a valid one, then the settlement server 8 approves the transaction (S306) and sends approval information to the settlement terminal (S307).

Industrial Applicability

As apparent from the above description, according to the present invention, terminal authentication is carried out through the use of a one-time password that is assigned to a terminal upon initial terminal information registration. As a result of the authentication, the terminal is provided with a terminal certificate encrypted according to an asymmetric algorithm. Thereafter, when settlement for a transaction is actually conducted, the terminal certificate and settlement information are encrypted on the basis of a symmetric algorithm, thereby obtaining a more reliable security effect.

Although the preferred embodiments of the present invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that various

modifications, additions and substitutions are possible, without departing from the scope and spirit of the invention as disclosed in the accompanying claims.

Claims:

1. A method for authenticating a settlement terminal connected to a settlement server over a network, comprising the steps of:

a) entering initial terminal information to said settlement server through said terminal and receiving a terminal ID and one-time password created by said settlement server;

b) gaining access to said settlement server through said terminal and sending said terminal ID and one-time password and a MAC (Media Access Control) address to said settlement server;

c) determining on the basis of the sent terminal ID, one-time password and MAC address that said terminal is an authorized one and then storing said terminal ID, one-time password and MAC address in said settlement server;

d) creating a terminal certificate for an SSL (Secure Socket Layer) protocol encrypted in an RSA (Rivest-Shamir-Adleman) manner on the basis of said terminal information and MAC address and storing the created terminal certificate in an LDAP (Light Weight Directory Access Protocol) server; and

e) sending said terminal information and terminal certificate, and a server certificate and SEED key created by a certificate authority to said terminal.

2. The method as set forth in claim 1, wherein said settlement server includes a terminal authentication server.

3. The method as set forth in claim 1, wherein said step a) includes the steps of:

a-1) connecting said terminal to said settlement server over said network;

a-2) entering a user ID and password for user identification;

a-3) sending said terminal information to said settlement server through said

terminal if a user is an authorized one;

a-4) storing the sent terminal information and creating said terminal ID and one-time password on the basis of the stored terminal information; and

a-5) storing the created terminal ID and one-time password and sending the stored terminal ID and one-time password and said MAC address to said terminal.

4. The method as set forth in claim 3, wherein the connection of said terminal to said settlement server is made by a manager.

5. The method as set forth in claim 1, wherein said one-time password is created in a challenge/response manner or time synchronous manner.

6. The method as set forth in claim 1, wherein said network is a TCP/IP-based network.

7. A settlement method based on authentication of a settlement terminal, comprising the steps of:

a) for settlement for a transaction, sending settlement information and a terminal certificate, encrypted on the basis of a SEED key, from said terminal to a settlement server according to an SSL (Secure Socket Layer) protocol over a network;

b) extracting a terminal certificate and terminal information stored in an LDAP (Light Weight Directory Access Protocol) server;

c) comparing a MAC (Media Access Control) address contained in said terminal certificate sent from said terminal with that contained in an information packet and, if the two MAC addresses are the same, determining that said terminal certificate sent from said terminal is valid;

d) comparing said terminal certificate sent from said terminal with said terminal certificate extracted from said LDAP server and authenticating said terminal if

the two terminal certificates are the same; and

e) approving said transaction on the basis of said settlement information and then sending approval information to said terminal.

8. The settlement method as set forth in claim 7, wherein said network is a TCP/IP-based network.

9. A settlement method based on authentication of a settlement terminal, comprising the steps of:

a) entering initial terminal information to a settlement server through said terminal and receiving a terminal ID and one-time password created by said settlement server;

b) gaining access to said settlement server through said terminal and sending said terminal ID and one-time password and a MAC (Media Access Control) address to said settlement server;

c) determining on the basis of the sent terminal ID, one-time password and MAC address that said terminal is an authorized one and then storing said terminal ID, one-time password and MAC address in said settlement server;

d) creating a terminal certificate for an SSL (Secure Socket Layer) protocol encrypted in an RSA (Rivest-Shamir-Adleman) manner on the basis of said terminal information and MAC address and storing the created terminal certificate in an LDAP (Light Weight Directory Access Protocol) server;

e) sending said terminal information and terminal certificate, and a server certificate and SEED key created by a certificate authority to said terminal;

f) for settlement for a transaction, allowing said terminal to encrypt settlement information and said terminal certificate with said SEED key and send the encrypted settlement information and terminal certificate to said settlement server;

g) receiving said terminal certificate and terminal information stored in said

LDAP server;

h) comparing a MAC address contained in said terminal certificate sent from said terminal with that contained in an information packet and, if the two MAC addresses are the same, determining that said terminal certificate sent from said terminal is valid;

i) comparing said terminal certificate sent from said terminal with said terminal certificate received from said LDAP server and authenticating said terminal if the two terminal certificates are the same; and

j) approving said transaction on the basis of said settlement information and then sending approval information to said terminal.

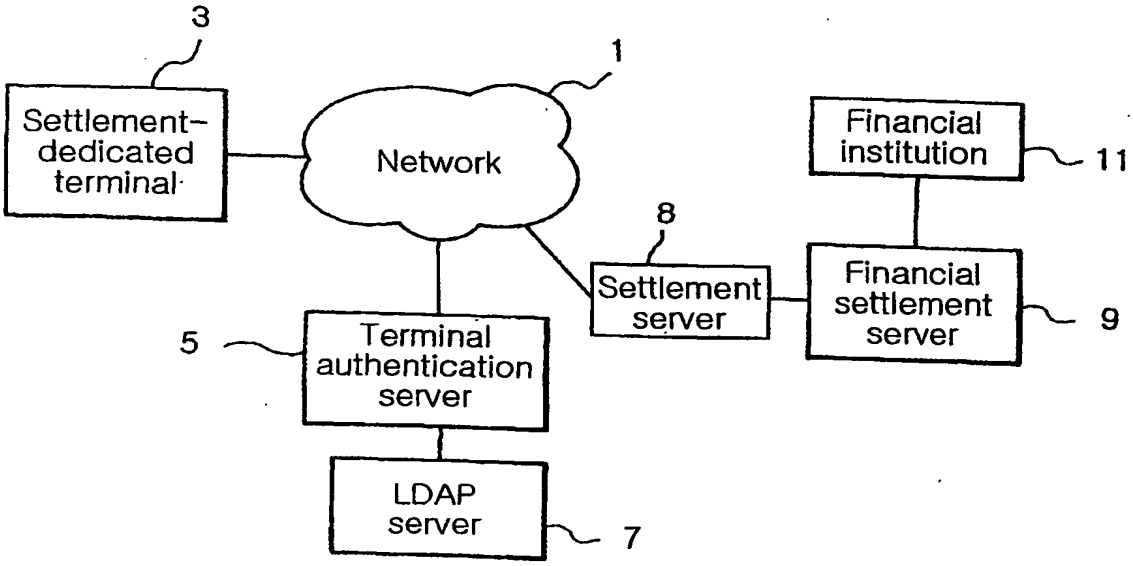

3
1
Settlement-dedicated terminal
Network
Financial institution
11
8
Settlement server
Financial settlement server
9
5
Terminal authentication server
LDAP server
7

FIG. 1

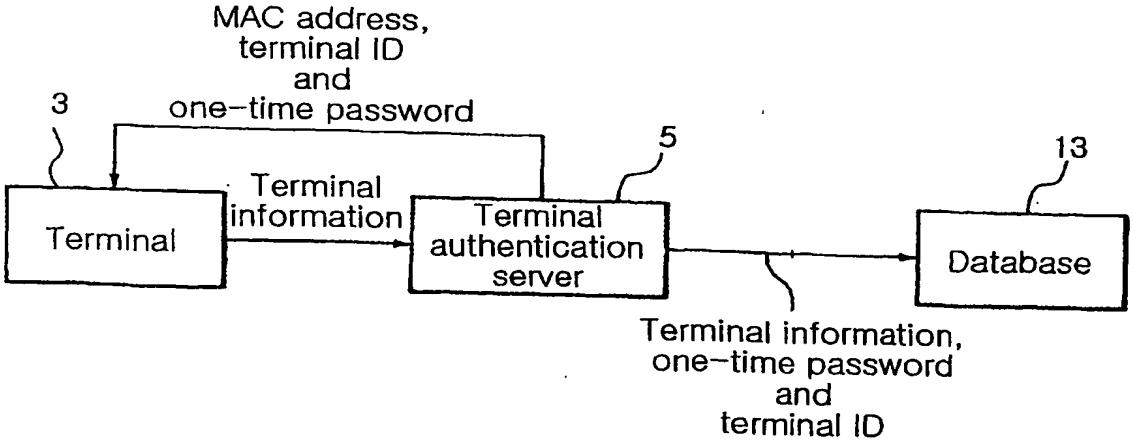

MAC address, terminal ID and one-time password
3
5
13
Terminal
Terminal information
Terminal authentication server
Database
Terminal information, one-time password and terminal ID

FIG. 2

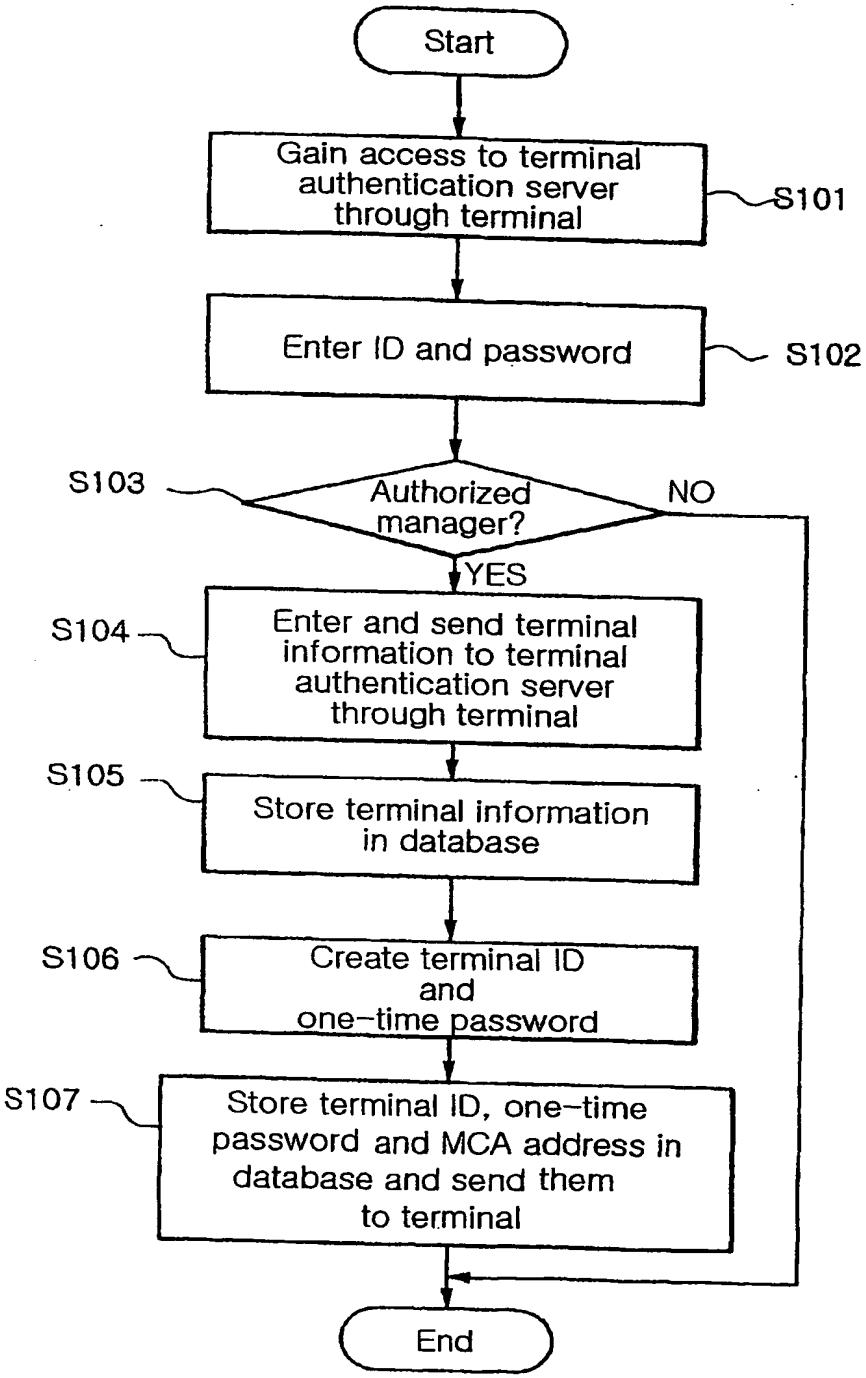

Start
Gain access to terminal authentication server through terminal
S101
Enter ID and password
S102
S103
Authorized manager?
NO
YES
S104
Enter and send terminal information to terminal authentication server through terminal
S105
Store terminal information in database
S106
Create terminal ID and one-time password
S107
Store terminal ID, one-time password and MCA address in database and send them to terminal
End

FIG. 3

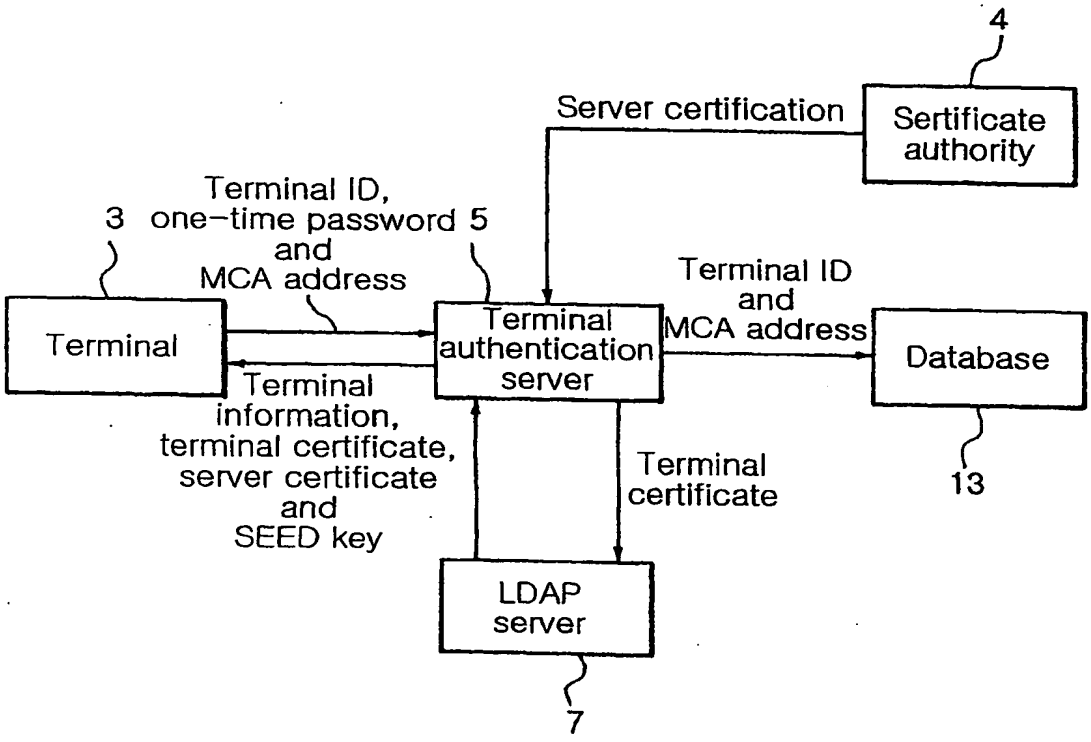

4
Server certification
Sertificate authority
Terminal ID, one-time password and MCA address
3
5
Terminal
Terminal authentication server
Terminal ID and MCA address
Database
Terminal information, terminal certificate, server certificate and SEED key
Terminal certificate
13
LDAP server
7

FIG. 4

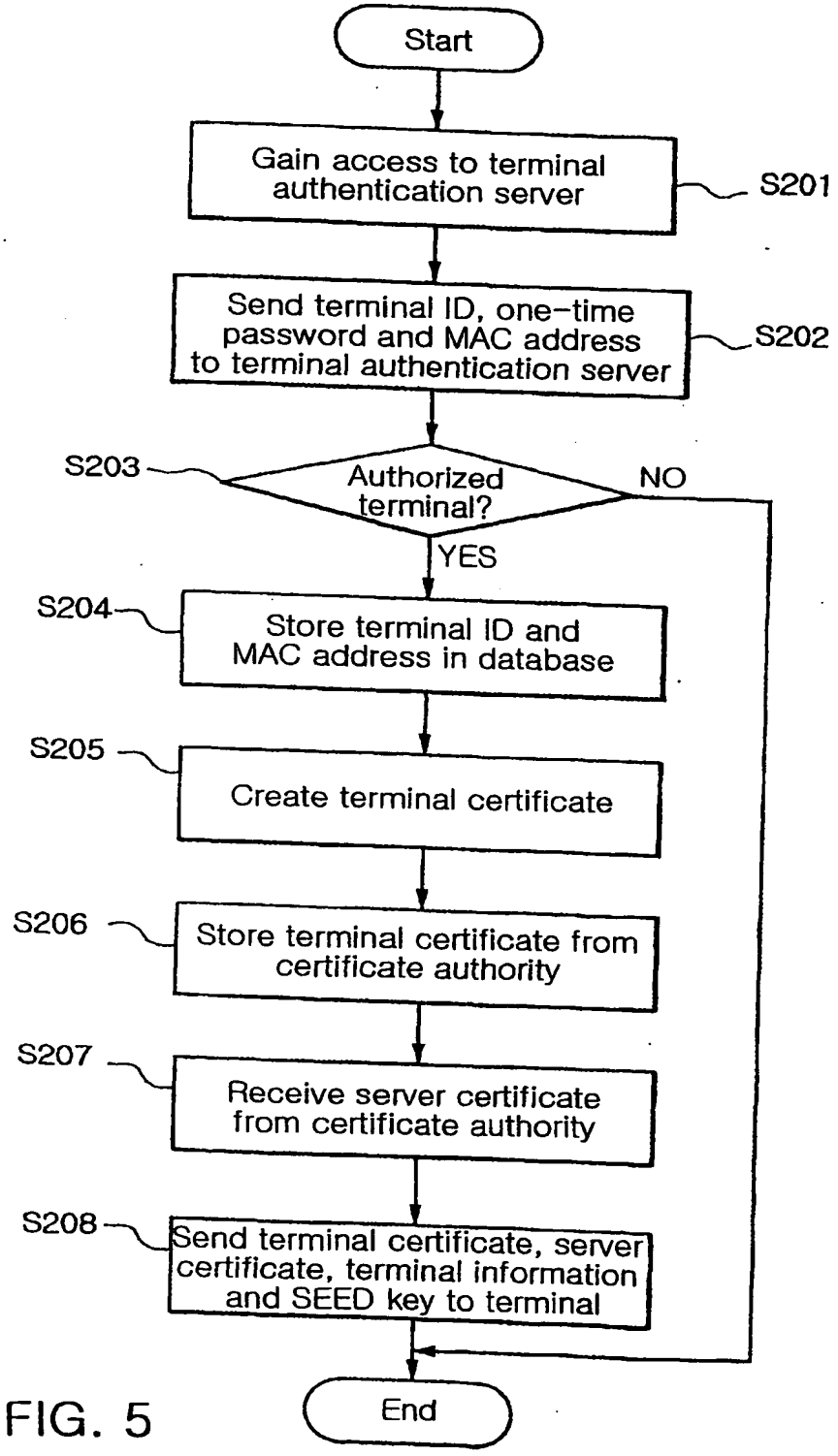

Start
Gain access to terminal authentication server
S201
Send terminal ID, one-time password and MAC address to terminal authentication server
S202
S203
Authorized terminal?
NO
YES
S204
Store terminal ID and MAC address in database
S205
Create terminal certificate
S206
Store terminal certificate from certificate authority
S207
Receive server certificate from certificate authority
S208
Send terminal certificate, server certificate, terminal information and SEED key to terminal
End

FIG. 5

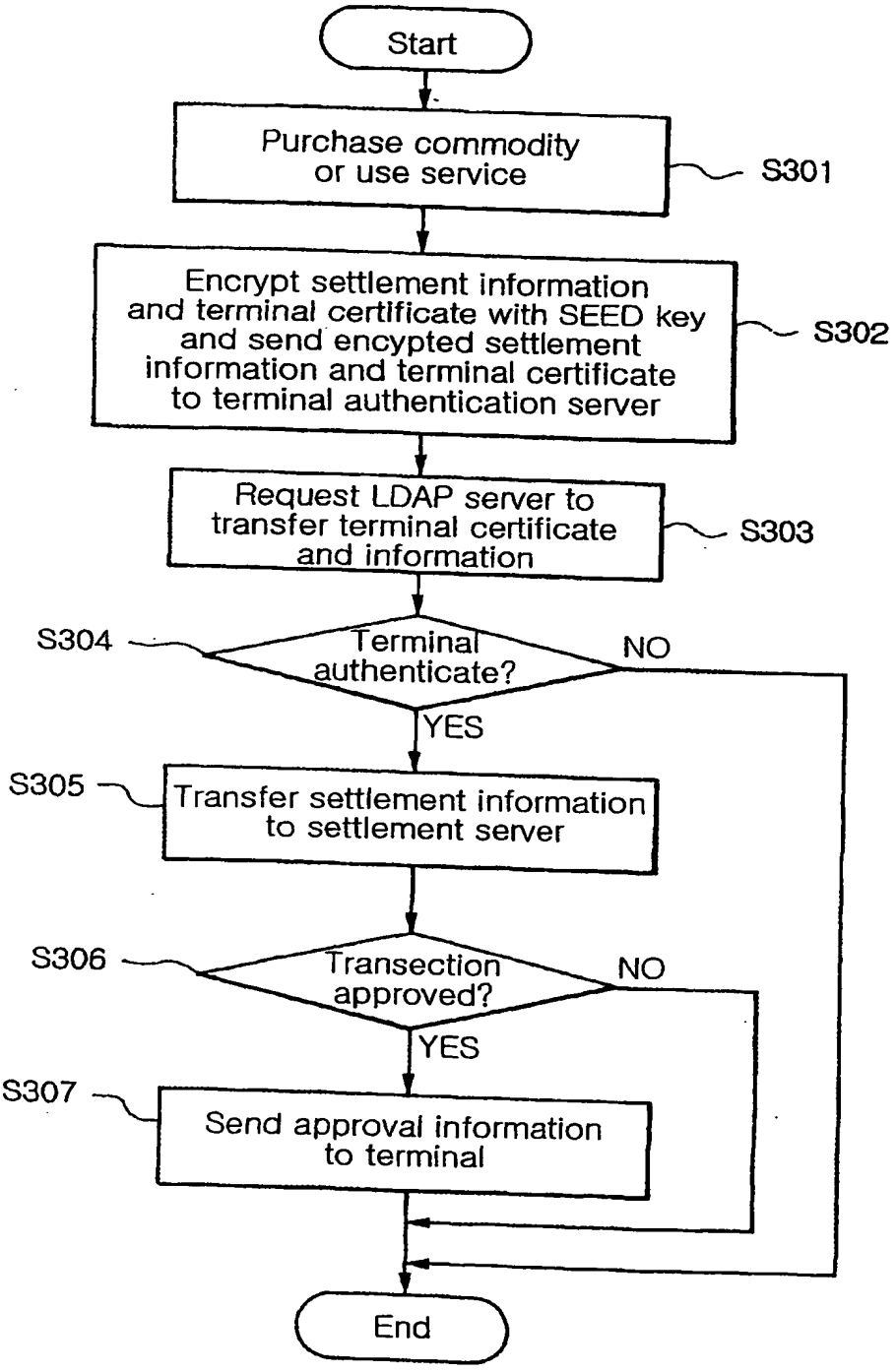

Start
Purchase commodity or use service
S301
Encrypt settlement information and terminal certificate with SEED key and send encypted settlement information and terminal certificate to terminal authentication server
S302
Request LDAP server to transfer terminal certificate and information
S303
S304
Terminal authenticate?
NO
YES
S305
Transfer settlement information to settlement server
S306
Transection approved?
NO
YES
S307
Send approval information to terminal
End

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR02/00288

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC7 H04L9 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
KR IPC as above

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)
FPD, USP, PAJ, IEL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-111544 A (NEC Corp) 20 April 2001 See column 【0017】 - 【0056】, Figure 3.	1 - 9
Y	JP 2000-201143 A (NEC Corp) 18 July 2000 See abstract, column 【0003】 - 【0009】.	1 - 9
A	A. Freier, P. Karlton and P. Kocher "The SSL Protocol, version 3.0, Internet Draft", March 1996, <http://home.netscape.com/eng/ssl3/ssl-toc.html> See the whole document.	1 - 9
A	US 5,668,876 A (Telefonaktiebolaget LM Ericsson) 16 Sep 1997 See abstract, column 5 line 21 - column 7 line 18.	1 - 9
A	KR 2000-0054777 (Shintel Corp) 5 Sep 2000 See the whole document.	1 - 9

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 JUNE 2002 (10.06.2002)	10 JUNE 2002 (10.06.2002)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	JEONG, Jae Heon Telephone No. 82-42-481-5672

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR02/00288

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2001- 111544 A	20-04-01	NONE	
US 5668876 A	16-09-97	WO 9600485 A	04-01-96
		JP 10502195 T	24-02-98
		FI 965161 A	13-02-97
		EP 766902 A	09-04-97
		AU 2688795 A	19-01-96
		CA 2193819 A	04-01-96
JP 2000-201143 A	18-07-00	NONE	
KR 2000-0054777 A	05-09-00	NONE	